

NON-LINEAR FEEDBACK SHIFT REGISTER CIRCUIT

Publication number: JP10320181

Publication date: 1998-12-04

Inventor: SHIMADA MICHIO

Applicant: NIPPON ELECTRIC CO

Classification:

- international: G06F7/58; G09C1/00; H03K3/84; H04L9/26; G06F7/58;
G09C1/00; H03K3/00; H04L9/18; (IPC1-7): G06F7/58;
G09C1/00; H03K3/84; H04L9/26

- European: G06F7/58P1

Application number: JP19970146072 19970521

Priority number(s): JP19970146072 19970521

Also published as:



EP0887728 (A2)

US6067359 (A1)

EP0887728 (A3)

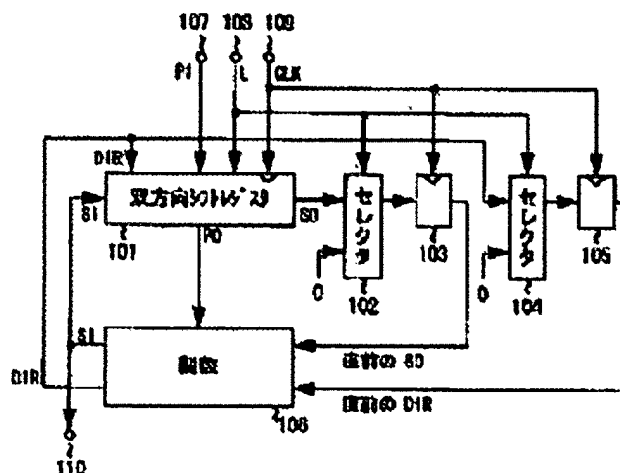
CA2238294 (C)

Report a data error here

Abstract of JP10320181

PROBLEM TO BE SOLVED: To attain a non-linear feedback shift register circuit allowed to be reduced at its circuit scale and easily designed.

SOLUTION: A bidirectional flip flop(FF) 101 shifts an internal state of m bits right or left in accordance with the value '0' or '1' of an output bit DIR from a function generator 106 and outputs a right end or left end bit as a serial output SO. The function generator 106 inputs a parallel output PO from the register 101, a just preceding serial output SO from the register 101 and a just preceding output bit DIR from the generator and outputs output bits SI, DIR. The output bit SI is outputted from an output terminal as a false random number. The design of the non-linear feedback shift register circuit is equivalent to the search of an Euler's function, the sorts of functions to be selected as main functions are various and the scale of the circuit can be reduced.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-320181

(43)公開日 平成10年(1998)12月4日

(51)Int.Cl. ⁸	識別記号	F I
G 0 6 F 7/58		G 0 6 F 7/58 A
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00 6 1 0 B
	6 5 0	6 5 0 B
H 0 3 K 3/84		H 0 3 K 3/84 Z
H 0 4 L 9/26		H 0 4 L 9/00 6 5 9
審査請求 有 請求項の数 5 F D (全 9 頁)		

(21)出願番号 特願平9-146072

(22)出願日 平成9年(1997)5月21日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

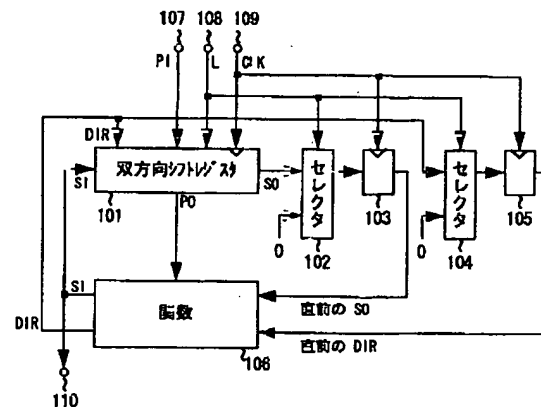
(74)代理人 弁理士 鈴木 康夫

(54)【発明の名称】 非線形フィードバック・シフトレジスタ回路

(57)【要約】

【課題】 回路規模の小型化が可能であり、かつ設計の容易な非線形フィードバック・シフトレジスタ回路を実現する。

【解決手段】 双方向フリップフロップ101は、関数発生器106の出力ビットDIRの値が0又は1に応じてmビットの内部状態を右又は左にシフトするとともに、右端又は左端のビットをシリアル出力SOとして出力する。関数発生器106は、双方向シフトレジスタ101の平行出力POと双方向シフトレジスタ101の直前のシリアル出力SOと関数発生器106の直前の出力ビットDIRを入力して、出力ビットSIと出力ビットDIRを出力する。出力ビットSIは疑似乱数として出力端子110から出力される。本発明の非線形フィードバック・シフトレジスタ回路の設計は、オイラー閉路を探索することと等価であり、主関数として選べる関数の種類が多様となり、かつ回路規模の小型化が可能である。



【特許請求の範囲】

【請求項1】 少なくとも、後述の関数発生器の第2の出力ビットの値が0あるいは1であるかに応じて、クロック信号が入力される毎に、保持されたmビットのビット系列を右あるいは左にシフトするとともに、ビット系列を右にシフトする際には、ビット系列の右端のビットをシリアル出力信号として出力して、前記関数発生器の第1の出力ビットをビット系列の左端に保持し、ビット系列を左にシフトする際には、ビット系列の左端のビットをシリアル出力として、前記関数発生器の第1の出力ビットをビット系列の右端に保持し、かつ、保持されているmビットのビット系列をパラレル出力信号として出力する双方方向シフトレジスタと、

前記クロック信号が入力される毎に前記双方方向シフトレジスタの前記シリアル出力信号を保持して保持された値を出力する第1のフリップフロップと、

前記クロック信号が入力される毎に前記関数発生器の第2の出力ビットを保持して保持された値を出力する第2のフリップフロップと、

前記双方方向シフトレジスタのパラレル出力信号と前記第1のフリップフロップの出力信号と前記第2のフリップフロップの出力信号に依存して第1の出力ビットと第2の出力ビットを出力する前記関数発生器と、から構成され、前記クロック信号が入力される毎に前記関数発生器の第1の出力ビットを疑似乱数として出力することとを特徴とする非線形フィードバック・シフトレジスタ回路。

【請求項2】 前記関数発生器は、前記双方方向シフトレジスタのパラレル出力信号に依存してそれぞれ1ビットを出力する第1の関数発生器および第2の関数発生器と、前記第1の関数発生器の出力と前記第1のフリップフロップの出力との排他的論理和を計算して計算結果を前記第1の出力ビットとして出力する第1の排他的論理和回路と、前記第2の関数発生器の出力と前記第2のフリップフロップの出力との排他的論理和を計算して計算結果を前記第2の出力ビットとして出力する第2の排他的論理和回路とから構成されていることを特徴とする請求項1記載の非線形フィードバック・シフトレジスタ。

【請求項3】 前記第1の関数発生器は、前記双方方向シフトレジスタのパラレル出力信号に依存してそれぞれ1ビットを出力する主関数発生器及び補助関数発生器と、この主関数発生器の出力と補助関数発生器の出力の排他的論理和を計算して計算結果を出力する排他的論理和回路とから構成されていることを特徴とする請求項2記載の非線形フィードバック・シフトレジスタ回路。

【請求項4】 前記主関数発生器は論理回路によって構成され、前記補助関数発生器は論理回路又はリード・オンリ・メモリ（ROM）によって構成されていることを特徴とする請求項3記載の非線形フィードバック・シフトレジスタ回路。

【請求項5】 前記各関数発生器の入力である前記双方

向シフトレジスタのパラレル出力データとそれに対応する前記各関数発生器の出力データを記録した請求項1、2、3又は4記載の非線形フィードバック・シフトレジスタに用いる記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信装置や情報処理装置において採用され、許可されていないものが通信データや記録媒体の内容を読みとることを困難にするために、送信データ系列に疑似乱数を排他的論理和で足し込む、ストリーム暗号を作成するための非線形フィードバック・シフトレジスタ回路に関するものである。

【0002】

【従来の技術】ストリーム暗号とは、送信データ系列に疑似乱数を排他的論理和で足し込むことによって、疑似乱数の値を知らない第三者によって送信データが読みとられることを防止するものである。

【0003】このストリーム暗号における疑似乱数を生成する方法として、非線形フィードバック・シフトレジスタ回路を用いる方法が古くから使われている。図9は、従来の非線形フィードバック・シフトレジスタ回路の基本構成を示す機能ブロック図である。

【0004】図9において、シフトレジスタ901は、入力端子908から供給される制御信号Lが0の時に入力端子909からクロック信号CLKが供給されると、入力端子907から供給されるmビットのビット列PIを内部状態として保持し、入力端子908から供給される制御信号Lが1の時に入力端子909からクロック信号CLKが供給されると、保持されている内部状態を右に1ビットシフトするとともに内部状態の左端には関数発生器902から供給されるシリアル入力SIが保持される。

【0005】シフトレジスタ901の内部状態は、パラレル出力POとして関数発生器902に供給される。また、関数発生器902の出力は、疑似乱数として出力端子910から出力される。関数発生器902は、リード・オンリ・メモリ（ROM）あるいは論理回路によって構成される。

【0006】図10は、シフトレジスタ901の基本構成を示す機能ブロック図である。図10において、セレクト1001₁～1001_mは、入力端子1005を介して供給される制御信号Lの値に応じてその左側から供給される2つの入力（上から順にA入力、B入力とする）の一方を選択して右側へ出力する。即ち、セレクト1001₁～1001_mは、制御信号Lが0であればA入力を選択して出力し、制御信号Lが1であればB入力を選択して出力する。

【0007】入力端子1007にはmビットのパラレル入力PIが供給され、PIのそれぞれのビットがセレクト1001₁～1001_mのA入力に供給される。また、

入力端子1008から供給されるシリアル入力SIが、セクタ1001₁のB入力に供給される。フリップフロップ1002₁～1002_{m-1}の出力は、セクタ1001₂～1001_mのB入力に供給される。フリップフロップ1002₁～1002_mは、入力端子1006からクロック信号CLKが供給される毎に、それぞれ図の左側のセクタ1001₁～1001_mの出力を保持して、保持した値を図の右側へ出力する。フリップフロップ1002₁～1002_mの出力は、mビットの平行出力POとして出力端子1010から出力される。したがって、シフトレジスタの内部状態はフリップフロップ1002₁～1002_mに保持されたビット系列によって表される。

【0008】シフトレジスタの内部状態を設定するには、まず内部状態として設定するmビットのデータを平行入力PIとして入力端子1007に供給し、入力端子1005に供給される制御信号Lを0とし、入力端子1006からクロック信号CLKを1個供給する。すると、平行入力PIの各ビットが対応するフリップフロップ1002₁～1002_mに保持される。

【0009】シフトレジスタに保持されたmビットを図の右方向に1ビットだけシフトするには、入力端子1005に供給される制御信号Lを1とする。そして、入力端子1006からクロック信号CLKを1個供給する。すると、シフトレジスタに保持されたmビットが図の右方向に1ビットだけシフトする。なお、その際には、入力端子1008から供給されたシリアル入力SIが左端のフリップフロップ1002₁に保持される。

【0010】図10のシフトレジスタの内部状態の可能な変化の仕方は、図11のような状態グラフによって表現することができる。図11は、m=3の場合のシフトレジスタの状態グラフである。図11において、丸印の中に書かれている3文字は、図9又は図10のシフトレジスタの内部状態を表している。丸印と丸印の間の矢印の付いた実線は状態の変化の方向を表しており、各実線に添えられている数字0又は1は、シフトレジスタの左端に供給されるシリアル入力SIの値を示している。また、矢印の付いた点線は状態が変化しないことを示している。

【0011】例えば、000が記入された丸印の右側に1があり、その数字の添えられている矢印の付いた実線の端に100が記入された丸印があるが、これはシフトレジスタのシリアル入力としてSI=1を供給してシフトレジスタを右にシフトさせると、シフトレジスタの内部状態が000から100に変化することを意味している。

【0012】これをグラフ理論における用語と対比させると、図の丸印がノードに対応し、実線が枝に対応している。したがって、従来の非線形フィードバック・シフトレジスタ回路を設計することは、図11の状態グラフ

においてハミルトン閉路を求めることに他ならない。ハミルトン閉路とは、全てのノードを1度だけ通過して元のノードに戻るような経路のことである。

【0013】関数発生器902の入力は、シフトレジスタ901の内部状態すなわち図11の丸印の内部の値であり、関数発生器902の出力はシフトレジスタ901に供給するシリアル入力SIすなわち図11の矢印の付いた実線に添えられた数字であるから、ハミルトン閉路が決まれば関数発生器902の入出力関係も決まる。

【0014】図12は、図11の状態グラフに存在するハミルトン閉路の一例である。図12において、小さな丸印で囲まれた数字の示す順序で、内部状態000から実線を矢印の方向にたどって行くと、全ての内部状態を1度だけ通過して、再び内部状態000に戻ることが分かる。

【0015】図13は、図12のハミルトン閉路に対応する関数発生器902の入出力対応を示した表である。図12の閉路の場合、関数発生器902から出力される疑似乱数の1周期の出力は、11101000となる。

【0016】なお、従来の非線形フィードバック・シフトレジスタ回路については、例えば、1986年にスプリング・ヴァーグから刊行されたルエベル著「アナリシス・アンド・デザイン・オブ・ストリーム・サイファ」(R.A.Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, 1986)などに詳しい解説がある。また、グラフ理論やハミルトン閉路については、例えば、高橋・藤重著「離散数学」(岩波書店1981年)などに詳しい解説がある。

【0017】

【発明が解決しようとする課題】しかしながら、従来の非線形フィードバック・シフトレジスタ回路は、その設計が難しいという問題があった。すなわち、前記のように、疑似乱数の周期を最大にするような関数を設計することは、ハミルトン経路を探索することに他ならないが、ハミルトン閉路を探索することは難しい問題であることが知られている(例えば、前記「離散数学」参照)。図11の例のように、ノードが8個しか存在しない場合には、試行錯誤で簡単に経路を発見することができるが、シフトレジスタの段数が大きくなってノードの数が多くなると、設計することは事実上不可能になる。

【0018】また、仮にハミルトン閉路を発見できたとしても、そのようなハミルトン閉路に対応する関数は、0と1とを等頻度で出力するから、論理圧縮して回路規模を小さくすることは、関数が線形な関数である場合など一部の例外を除けば一般に困難である。

【0019】本発明は、以上の問題点を鑑み、設計が容易で、かつ回路規模を小さくすることができる非線形フィードバック・シフトレジスタ回路を提供することを目的とするものである。

【0020】

【課題を解決するための手段】本発明は、双方向にシフトできるシフトレジスタ（以下、双方向シフトレジスタという）を用いて非線形フィードバック・シフトレジスタ回路を構成したことを特徴とするものである。

【0021】グラフの全ての枝をそれぞれ1度だけ通るような経路は、オイラー経路と呼ばれ、探索することが容易であることが知られている。より厳密に言うと、もし、グラフのノードから出ている枝の数が、どのノードについても2あるいは4であれば、グラフの全ての枝をそれぞれ1度だけ通るような経路が存在し、しかも、そのような経路は簡単に求められることが知られている。これらのことについては、グラフ理論関係の参考書（例えば前記の文献等参照）に詳しい解説がある。

【0022】後述するように、双方向シフトレジスタを利用して非線形フィードバック・シフトレジスタ回路を設計することは、前記オイラー閉路を探索することに帰着され、よって、非線形フィードバック・シフトレジスタ回路の設計が容易となる。

【0023】

【発明の実施の形態】図1は、本発明の非線形フィードバック・シフトレジスタの第1の実施の形態を示す機能ブロック図であり、図2は、本発明において用いられる双方向シフトレジスタの基本構成を示す機能ブロック図である。

【0024】説明の便宜上、最初に双方向シフトレジスタについて説明する。図2において、セクタ201₁～201_mは、入力端子204から供給される制御信号DIR及び入力端子205から供給される制御信号Lの各値に応じて、図の左側から供給される3つの入力（図の上から順にA入力、B入力、C入力とする）を選択し、選択された入力を図の右側へ出力する。セクタ203は、入力端子204から供給される制御信号DIRの値に応じて、図の左側から供給される2つの入力（図の上から順にB入力、C入力とする）を選択し、選択された入力をシリアル出力SOとして出力端子209から出力する。

【0025】セクタ201₁～201_mは、制御信号Lが0であればA入力を選択して出力し、制御信号Lが1で制御信号DIRが0であればC入力を選択して出力し、制御信号Lが1で制御信号DIRが1であればB入力を選択して出力する。セクタ203は、制御信号DIRが0であればC入力を選択して出力し、制御信号DIRが1であればB入力を選択して出力する。

【0026】入力端子207にはmビットの平行入力PIが供給され、PIのそれぞれのビットがセクタ201₁～201_mのA入力に供給される。また、入力端子208から供給されるシリアル入力SIが、セクタ201₁のB入力とセクタ201_mのC入力に供給される。

【0027】フリップフロップ202₁～201_mは、入

力端子206からクロック信号CLKが供給される毎に、それぞれ図の左側のセクタ201₁～201_mの出力を保持して、保持した値を図の右側へ出力する。フリップフロップ202₁～201_mから出力される合計mビットの出力は、平行出力POとして、出力端子210から出力される。

【0028】m-1個のフリップフロップ202₁～202_{m-1}の出力は、それぞれ図の右側のセクタ201₂～201_mのB入力にも供給されている。フリップフロップ202_mの出力は、セクタ203のB入力にも供給されている。m-1個のフリップフロップ202₂～202_mの出力は、それぞれ図の左側のセクタ201₁～201_{m-1}のC入力にも供給されている。フリップフロップ202₁の出力は、セクタ203のC入力にも供給されている。双方向シフトレジスタの内部状態は、フリップフロップ202₁～202_mに保持されたビット系列によって表される。

【0029】双方向シフトレジスタの内部状態を設定するには、内部状態として設定するmビットのデータを平行入力PIとして入力端子207に供給するとともに入力端子205に供給される制御信号Lを0とし、入力端子206からクロック信号CLKを1個供給する。すると、平行入力PIのビットが、それぞれフリップフロップ202₁～202_mに保持される。

【0030】双方向シフトレジスタに保持されたmビットを図の右方向に1ビットだけシフトするには、まず、入力端子205に供給される制御信号Lを1とし、入力端子204に供給される制御信号DIRを1とする。その際には、セクタ203はB入力を選択するので右端のフリップフロップ202_mに保持されていたビットがシリアル出力SOとして出力端子209から出力される。そして、入力端子206からクロック信号CLKを1個供給すると、双方向シフトレジスタに保持されたmビットが図の右方向に1ビットだけシフトするとともに入力端子208から供給されたシリアル入力SIが左端のフリップフロップ202₁に保持される。

【0031】双方向シフトレジスタに保持されたmビットを図の左方向に1ビットだけシフトするには、まず、入力端子205に供給される制御信号Lを1とし、入力端子204に供給される制御信号DIRを0とする。その際には、セクタ203はC入力を選択するので左端のフリップフロップ202₁に保持されていたビットがシリアル出力SOとして出力端子209から出力される。そして、入力端子206からクロック信号CLKを1個供給すると、双方向シフトレジスタに保持されたmビットが図の左方向に1ビットだけシフトするとともに入力端子208から供給されたシリアル入力SIが右端のフリップフロップ202_mに保持される。

【0032】図5は、図2の双方向シフトレジスタの状態グラフをm=3の場合について表したものである。図

5において、丸印の中に書かれている3ビットは、図2の双方向シフトレジスタのフリップフロップに保持されているビットを表している。そして、丸印と丸印が、両端に矢印の付いた実線で結ばれている。また、どの実線の両端にも、1R、1L、0R、0Lの4通りの記号の何れかが添えられている。

【0033】この状態グラフの見方は、例えば、000が記入された丸印の右側に、1Rと言う記号があり、その記号が添えられている実線のもう一方の端に100が記入された丸印があるが、1Rの1はシリアル入力SIの値を示し、1RのRは右シフトを示しており、これは、SI=1として双方向シフトレジスタを右にシフトさせると、双方向シフトレジスタの内部状態が000から100に変化することを意味している。

【0034】図5の状態グラフは、内部状態000、111に対応するノードからは2本の枝が出ており（同じノードに戻る枝を無視すれば）、それ以外のノードからは4本の枝が出ているので、オイラー閉路が存在する。図6は、図5の状態グラフに存在するオイラー閉路の1例である。図において、小さな丸印で囲まれた数字の示す順序で、内部状態000から実線を進んで行くと、全ての実線を進んで、再び内部状態000に戻ることが分かる。

【0035】図1において、双方向シフトレジスタ101は、前記のように、入力端子108から供給される制御信号Lが0の時に入力端子109からクロック信号CLKが供給されると、入力端子107から供給されるmビットの平行入力PIを内部状態として保持し、入力端子108から供給される制御信号Lが1で関数発生器106が出力する制御信号DIRが1の時には、内部状態の右端のビットをシリアル出力SOとしてセレクト102に供給し、その時に、入力端子109からクロック信号CLKが供給されると、内部状態を右に1ビットだけシフトして、内部状態の左端にシリアル入力SIを保持し、入力端子108から供給される制御信号が1で関数発生器106の出力する制御信号DIRが0の時には、内部状態の左端のビットをシリアル出力SOとしてセレクト102に供給し、その時に、入力端子109からクロック信号CLKが供給されると、内部状態を左に1ビットだけシフトして、内部状態の右端にシリアル入力SIを保持する。

【0036】また、双方向シフトレジスタ101の内部状態は平行出力POとして関数発生器106に供給される。セレクト102は、入力端子108から供給される制御信号Lが0の時には0を選択して出力し、制御信号Lが1の時には、双方向シフトレジスタ101から供給されるシリアル出力SOを選択して出力し、その出力をフリップフロップ103に供給する。フリップフロップ103は、入力端子109からクロック信号CLKが供給されると、セレクト102の出力を保持して、保

持したビットを関数発生器106に供給する。

【0037】セレクト104は、入力端子108から供給される制御信号Lが0の時には0を選択して出力し、制御信号Lが1の時には、関数発生器106が出力する制御信号DIRを選択して出力し、その出力をフリップフロップ105に供給する。フリップフロップ105は、入力端子109からクロック信号CLKが供給されると、セレクト104の出力を保持して、保持したビットを関数発生器106に供給する。

【0038】関数発生器106は、双方向シフトレジスタ101から出力される平行出力POと、フリップフロップ103及び105の出力に依存して、制御信号SIと制御信号DIRを出力する。また、関数発生器106の出力する制御信号SIは、疑似乱数として、出力端子110から出力される。

【0039】なお、フリップフロップ103の出力は、1時刻前、すなわち、入力端子109からクロック信号CLKが入力される前に、双方向シフトレジスタ101が出力していたシリアルデータSOであり、フリップフロップ105の出力は、1時刻前に、関数発生器105が出力していた制御信号DIRである。双方向シフトレジスタ101は、1時刻に1ビットだけしかシフトされないから、それらのデータだけで、双方向シフトレジスタ101の1時刻前の状態が特定できる。このため、双方向シフトレジスタの平行出力POと、1時刻前のSO及びDIRだけに依存して、関数発生器106の出力SIとDIRが決定される。

【0040】次に、本発明の非線形フィードバック・シフトレジスタの動作について説明する。最初に、双方向シフトレジスタ101の内部状態の初期状態として設定するmビットのデータを平行入力PIとして入力端子107に供給し、入力端子108に供給される制御信号Lを0とし、入力端子109からクロック信号を1個供給する。次に入力端子108に供給される制御信号Lを1とする。するとそれ以降は、入力端子109からクロック信号CLKが1個供給される毎に、出力端子110から疑似乱数のビットが出力される。

【0041】ただし、双方向シフトレジスタ101の内部状態の初期状態を000あるいは111にすると、関数によっては、それ以降の内部状態がずっと000あるいは111になって、内部状態がオイラー閉路に沿って遷移しなくなる。例えば図6の例では、内部状態の初期状態を000にしてしまうと、それ以降の内部状態はずっと000のみである。このため、図1の実施の形態においては、双方向シフトレジスタ101の内部状態の初期状態をオール0やオール1にすることは避ける必要がある。

【0042】関数発生器106は、リード・オンリ・メモリ（ROM）あるいは論理回路によって構成することができる。例えば、図6のオイラー閉路に対応する状態

遷移を実現するには、関数発生器106の入力と出力の関係を図7の表のように設定すればよい。双方向シフトレジスタ101の内部状態の初期状態によっては図6の実線に添えられて番号と逆順に進むこともあるが、いずれの場合も、初期状態を000あるいは111にしない限り、オイラー閉路に沿って移動する。

【0043】図3は、本発明の非線形フィードバック・シフトレジスタの第2の実施の形態を示す機能ブロック図である。この実施の形態においては、関数発生器106の構成方法が前記第1の実施の形態と異なっているだけで、他の部分は第1の実施の形態と同様である。すなわち、図3においては、フリップフロップ103と105の出力が、関数発生器106ではなく、それぞれ排他的論理和回路303と304に供給されている。

【0044】排他的論理和回路303においては、フリップフロップ103の出力と関数発生器301の出力 f との排他的論理和が計算され、その計算結果は制御信号SIおよび疑似乱数出力として出力される。また、排他的論理和回路304においては、フリップフロップ105の出力と関数発生器302の出力 d との排他的論理和が計算され、その計算結果は制御信号DIRとして出力される。双方向シフトレジスタ101から出力されるパラレルデータPOは、関数発生器301と302にそれぞれ供給される。

【0045】関数発生器301と302は、それぞれリード・オンリ・メモリ（ROM）あるいは論理回路によって構成される。そして、例えば図6のオイラー閉路に対応する状態遷移を実現する場合には、各関数発生器の出力 f と d を、図8の入出力対応表のように設定すればよい。このようにすれば、図3の双方向シフトレジスタの内部状態は、図6のオイラー閉路に沿って移動する。双方向シフトレジスタ101の内部状態の初期状態によっては図6に実線に添えられた番号とは逆順に進むこともあるが、いずれの場合もオイラー閉路に沿って移動する。

【0046】これは、どのようなオイラー閉路についても、内部状態Sに対して2つのビットSI(S)、DIR(S)が存在して、 $SI = \text{「直前のSO」} + SI(S)$ 、 $DIR = \text{「直前のDIR」} + DIR(S)$ という関係が成り立っていることに依るものである。ここで、+は排他的論理和を意味する。この関係は図7の入出力対応表においても成り立っているこの第2の実施の形態においては、図8に示すように、その入出力対応表は、図7に示す第1の実施の形態における入出力対応表よりも簡単化することができるので、関数発生器をROMで構成した場合には、メモリ容量を小さくすることができる。また、論理回路で構成した場合には、関数の入力ビット数が少なくなり、回路規模を小さくすることができるとともに、動作に伴う遅延時間も小さくなる。

【0047】図4は、第2の実施の形態における関数発

生器301の一例を示すブロック図である。図4において、入力端子404から入力されたパラレルデータPOは、主関数発生器401と補助関数発生器402に入力される。主関数発生器401は論理回路によって構成され、その入力に依存して1ビットを出力する。補助関数発生器402は、ROMあるいは論理回路によって構成され、その入力に依存して1ビットを出力する。そして、主関数発生器401の出力と補助関数発生器402の出力との排他的論理和が排他的論理和回路403で計算され、計算結果が出力端子405から関数の出力として出力される。

【0048】図4の関数発生器を構成するにあたっては、まず、オイラー閉路を選択する前に、主関数発生器401を構成する論理回路を適当に決めておく。その際に、論理回路として回路規模の小さな論理回路を選択する。そして、補助関数発生器402と関数発生器302の出力ができるだけ0となるようなオイラー閉路を選択する。出力の大部分が0であるような論理回路であれば、論理圧縮することで回路規模あるいはメモリ容量を小さくすることができる。一般に、 m 段の双方向シフトレジスタの状態グラフには、3の $2^m - 2$ 乗通りのオイラー閉路が存在することが知られており、上記のような条件を満たすオイラー閉路は高い確率で見える。

【0049】

【発明の効果】本発明は、双方向シフトレジスタを用い、非線形フィードバック・シフトレジスタの設計を、オイラー閉路によって実現しており、かつオール0とオール1以外の任意のバイナリ系列を初期状態として設定できるので、回路設計が容易である。

【0050】また、双方向シフトレジスタを用いているにもかかわらず、関数発生器の構成を工夫することにより、回路規模を小さくすることができる。

【0051】さらに、関数として選べる種類が非常に多いので、ストリーム暗号の解読が困難な疑似乱数を多く生成することができ、主関数を秘密にすることによる暗号強度の増加を図ることができる。

【0052】

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示す機能ブロック図である。

【図2】双方向シフトレジスタの基本構成を示す機能ブロック図である。

【図3】本発明の第2の実施の形態を示す機能ブロック図である。

【図4】本発明の第2の実施の形態において用いられる複数の関数発生器のうちの一つを示す機能ブロック図である。

【図5】 $m = 3$ の場合の双方向シフトレジスタの状態グラフである。

【図6】図5の状態グラフに存在するオイラー閉路の一

例を示す図である。

【図7】第1の実施の形態における関数発生器に対する図6のオイラー閉路の場合の入出力対応表である。

【図8】第2の実施の形態における関数発生器に対する図6のオイラー閉路の場合の入出力対応表である。

【図9】従来の非線形フィードバック・シフトレジスタ回路を示す機能ブロック図である。

【図10】シフトレジスタに基本構成を示す機能ブロック図である。

【図11】 $m=3$ の場合のシフトレジスタの状態グラフである。

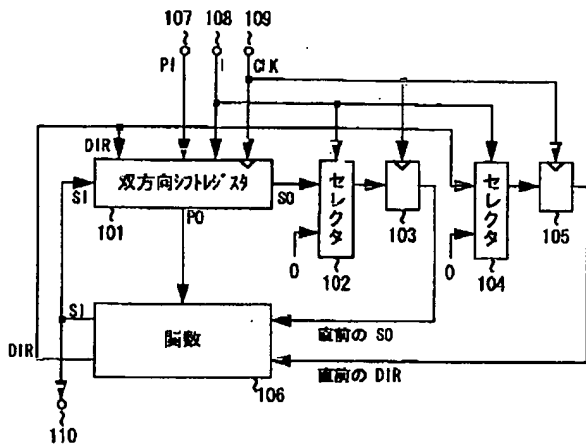
【図12】図11の状態グラフに存在するハミルトン閉路の一例を示す図である。

【図13】従来例における関数発生器に対する図12のハミルトン閉路の場合の入出力対応表である。

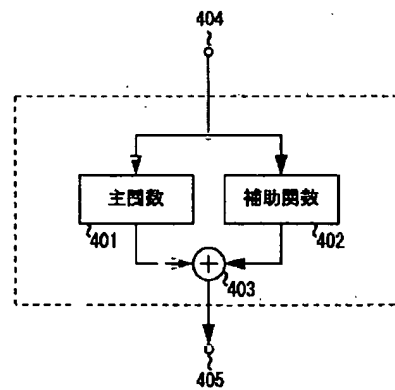
【符号の説明】

- 101 双方向シフトレジスタ
 102, 104, 201, 203, 1001 セレクタ
 103, 105, 202, 1002 フリップフロップ
 106 関数発生器
 301 第1の関数発生器
 302 第2の関数発生器
 401 主関数発生器
 402 補助関数発生器
 303, 304, 403 排他的論理和回路
 901 シフトレジスタ
 902 関数発生器

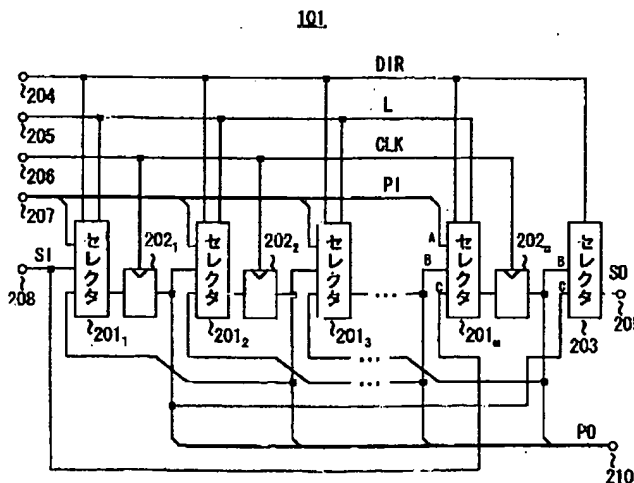
【図1】



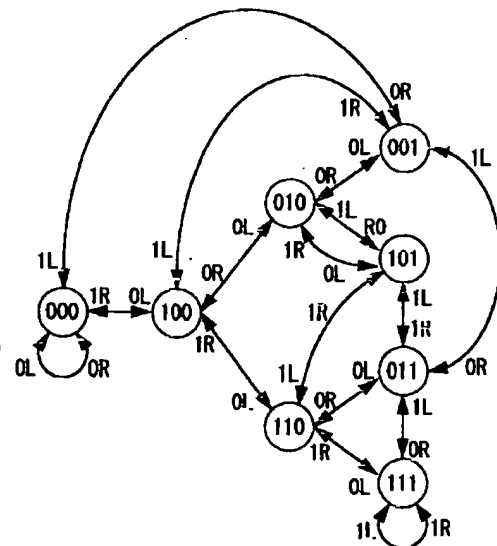
【図4】



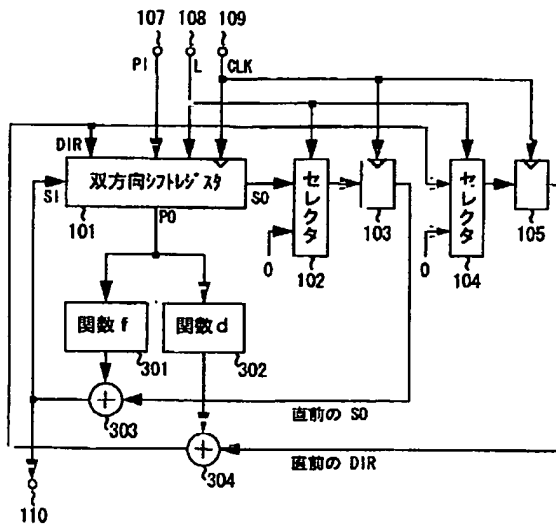
【図2】



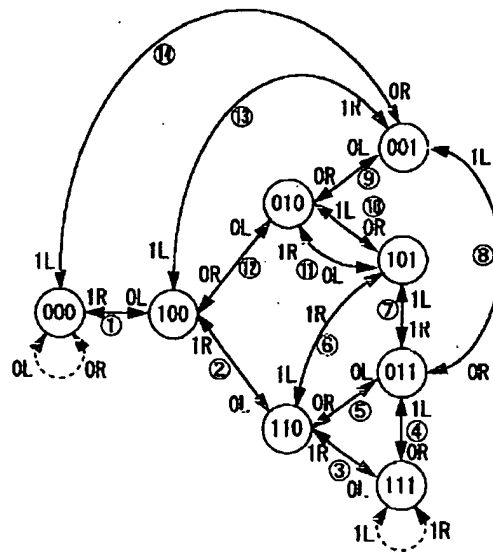
【図5】



【図3】



【図6】



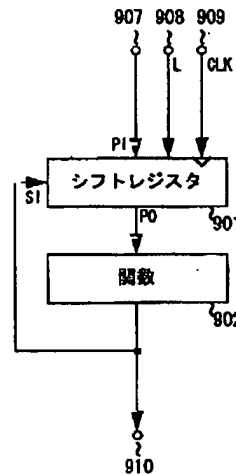
【図7】

P0	直前のS0	直前のDIR	SI	DIR
000	1	1 (R)	1	1 (R)
000	1	0 (L)	1	0 (L)
001	1	1 (R)	0	0 (L)
001	1	0 (L)	0	1 (R)
001	0	1 (R)	1	0 (L)
001	0	0 (L)	1	1 (R)
010	1	0 (L)	0	0 (L)
010	0	0 (L)	1	0 (L)
010	1	1 (R)	0	1 (R)
010	0	1 (R)	1	1 (R)
011	1	1 (R)	0	0 (L)
011	1	0 (L)	0	1 (R)
011	0	1 (R)	1	0 (L)
011	0	0 (L)	1	1 (R)
100	0	1 (R)	1	1 (R)
100	0	0 (L)	1	0 (L)
100	1	0 (L)	0	0 (L)
100	1	1 (R)	0	1 (R)
101	1	0 (L)	1	0 (L)
101	0	0 (L)	0	0 (L)
101	1	1 (R)	1	1 (R)
101	0	1 (R)	0	1 (R)
110	0	1 (R)	1	1 (R)
110	0	0 (L)	1	0 (L)
110	1	0 (L)	0	0 (L)
110	1	1 (R)	0	1 (R)
111	0	1 (R)	0	1 (R)
111	0	0 (L)	0	0 (L)

【図8】

P0	f	d
000	0	0
001	1	1
010	1	0
011	1	1
100	1	0
101	0	0
110	1	0
111	0	0

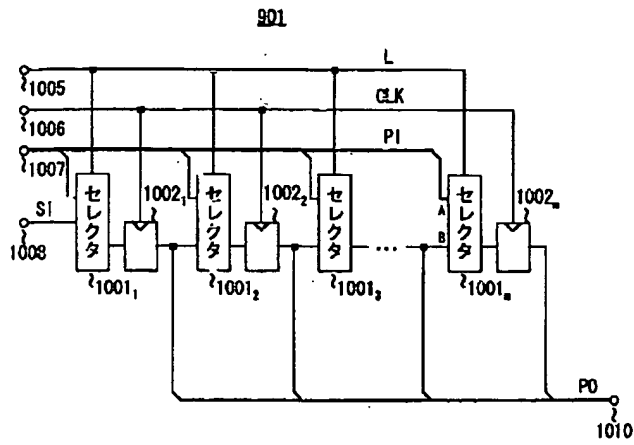
【図9】



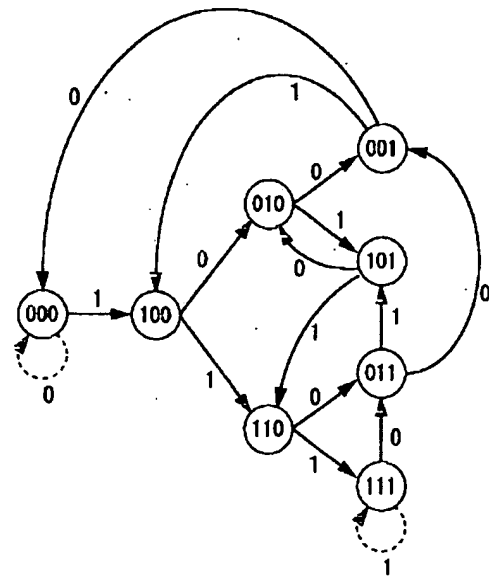
【図13】

P0	関数の出力
000	1
001	0
010	0
011	1
100	1
101	0
110	1
111	0

【図10】



【図11】



【図12】

